Leitfaden für Netzwerkarchitekten zur Einführung eines Zero Trust-Netzwerkzugriff-Service

Best Practices für die Verwendung von ZTNA als VPN-Alternative

zscaler™

Angesichts der Verlagerung privater Anwendungen in die Cloud und der Zunahme von Benutzern, die an weltweit verteilten Standorten arbeiten, benötigen Unternehmen einen Service, der den sicheren Zugriff auf private Apps ermöglicht und gleichzeitig eine reibungslose Nutzererfahrung bietet. Obwohl alle Welt aufgeregt die Vorteile der Zero-Trust-Sicherheit diskutiert, versuchen einige Unternehmen, herkömmliche netzwerkzentrierte Architekturen mit Firewalls der nächsten Generation auszustatten, um die Konnektivität der Benutzer mit Anwendungen zu beschränken. Diese herkömmlichen Architekturen entsprechen jedoch nicht mehr den heutigen Anforderungen und wurden nicht dafür entwickelt, autorisierte Benutzer mit bestimmten Anwendungen zu verbinden. Sie erzwingen die Platzierung der Benutzer im Netzwerk und laufen damit häufig Gefahr, Lateralbewegungen zu anderen Apps zu ermöglichen und IP-Adressen im Internet zu exponieren sowie zu DDoS-Angriffen über VPN-Konzentratoren, die am Rand des Netzwerks auf eingehende Pings warten, geradezu einzuladen.

Viele Unternehmen erwägen ZTNA-Services (Zero Trust Network Access) als Alternative zu VPN. Tatsächlich geht Gartner davon aus, dass bis zum Jahr 2021 60% der Unternehmen ihr bestehendes VPN nach und nach zugunsten eines ZTNA-Service auslaufen lassen werden. In der Praxis kann sich allerdings in großen (globalen) Organisationen selbst eine kleine Veränderung der Art und Weise, wie Benutzer auf Anwendungen zugreifen, zu einer gewaltigen Aufgabe auswachsen. Dieses Dokument hilft Ihnen dabei, zu verstehen, wo Sie am besten ansetzen, damit Sie ZTNA schnell und möglichst ohne Unterbrechungen des laufenden Geschäfts einführen können.

In diesem Leitfaden werden wir folgende Aspekte behandeln:

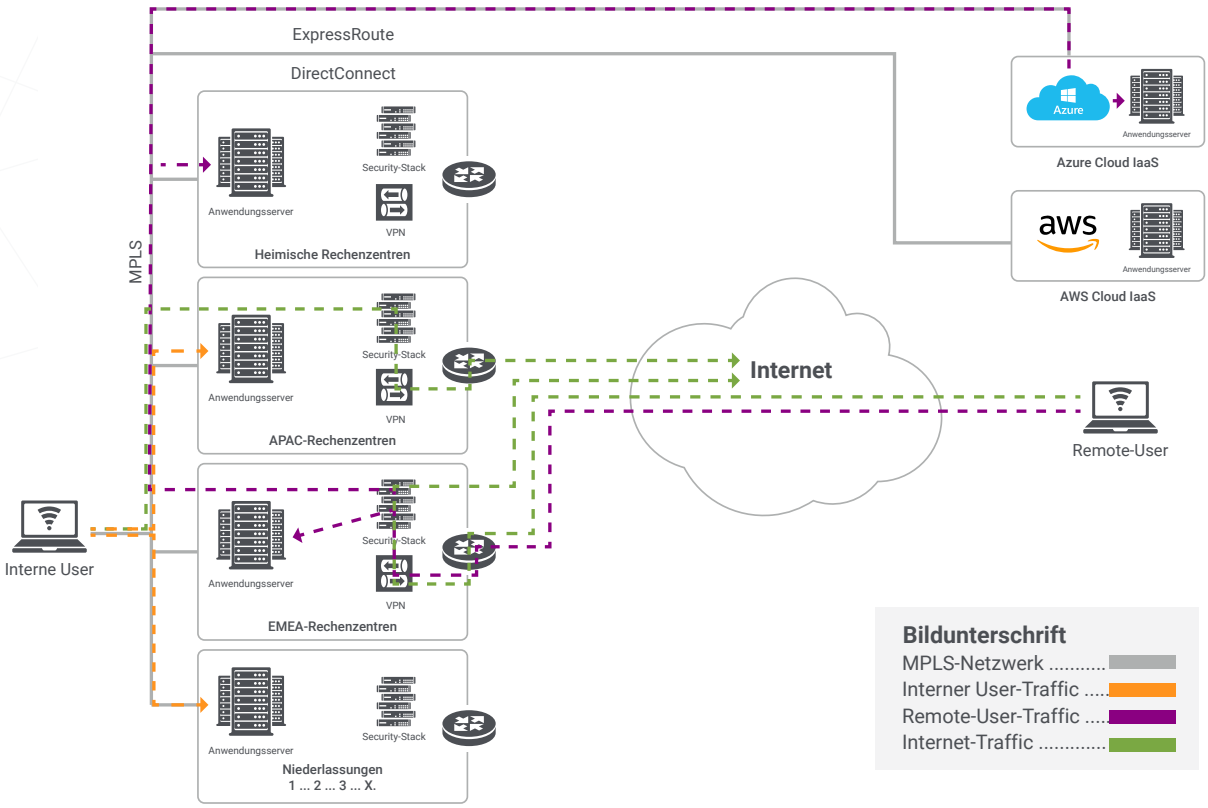
- Unterschiede in der Architektur herkömmlicher Zugangstechnologien und ZTNA.
- Eine Referenzarchitektur für die Bereitstellung von ZTNA.
- Die drei Phasen, die Sie bei der Einführung von ZTNA in Ihrem Unternehmen beachten müssen.
- Profi-Tipps und Erwägungen zur optimalen Nutzung Ihres ZTNA-Deployment.

Bevor wir beginnen, nehmen Sie sich doch bitte einen Moment Zeit und lesen Sie den Blog “Mitigating Risk via the Software-defined Perimeter.” („Risiken mithilfe des Software Defined Perimeter minimieren“). Dieser Blogbeitrag verschafft Ihnen einen ersten Überblick über vertrauenswürdige ZTNA-Services.

Jetzt werden wir uns jedoch näher damit beschäftigen, wie man mit der ZTNA-Architektur autorisierte Benutzer mit bestimmten privaten Anwendungen verbinden kann, ohne sie im Netzwerk zu platzieren.

Wo stehen Sie derzeit? - VPN im Unternehmen

Die Architektur, die man für gewöhnlich in Organisationen vorfindet, ist in dieser Übersichtsgrafik dargestellt. Ich bin mir durchaus bewusst, dass die Anzahl und Anordnung der Rechenzentren, Router, Firewalls, VPN-Konzentratoren und des MPLS-Netzwerks in der Praxis nicht unbedingt mit dieser Abbildung übereinstimmen. Für unsere Zwecke betrachte ich die Abbildung der Komponenten jedoch als ausreichend. Natürlich werden in Organisationen viele andere Netzwerk- und Sicherheitsvorrichtungen eingesetzt, darunter Inline-Proxys, Sandboxes, L7-Firewalls, AV- und DLP-Lösungen usw. Im Sinne einer vereinfachten Darstellung habe ich jedoch das gesamte Internet-Sicherheitskonzept in den Abbildungen unter Security-Stack zusammengefasst.



Auf einige Punkte dieser traditionellen Architektur möchte ich besonders hinweisen:

01 Remote-User werden über VPN mit einem der Rechenzentren verbunden und in das Unternehmensnetzwerk eingebunden. Meiner Erfahrung nach, ist das Netzwerk bei vielen Organisationen relativ flach, und die ACLs sind eher begrenzt. Das macht die gesamte Infrastruktur und die Netzwerke des Unternehmens-Rechenzentrums für alle Remote-User sichtbar.

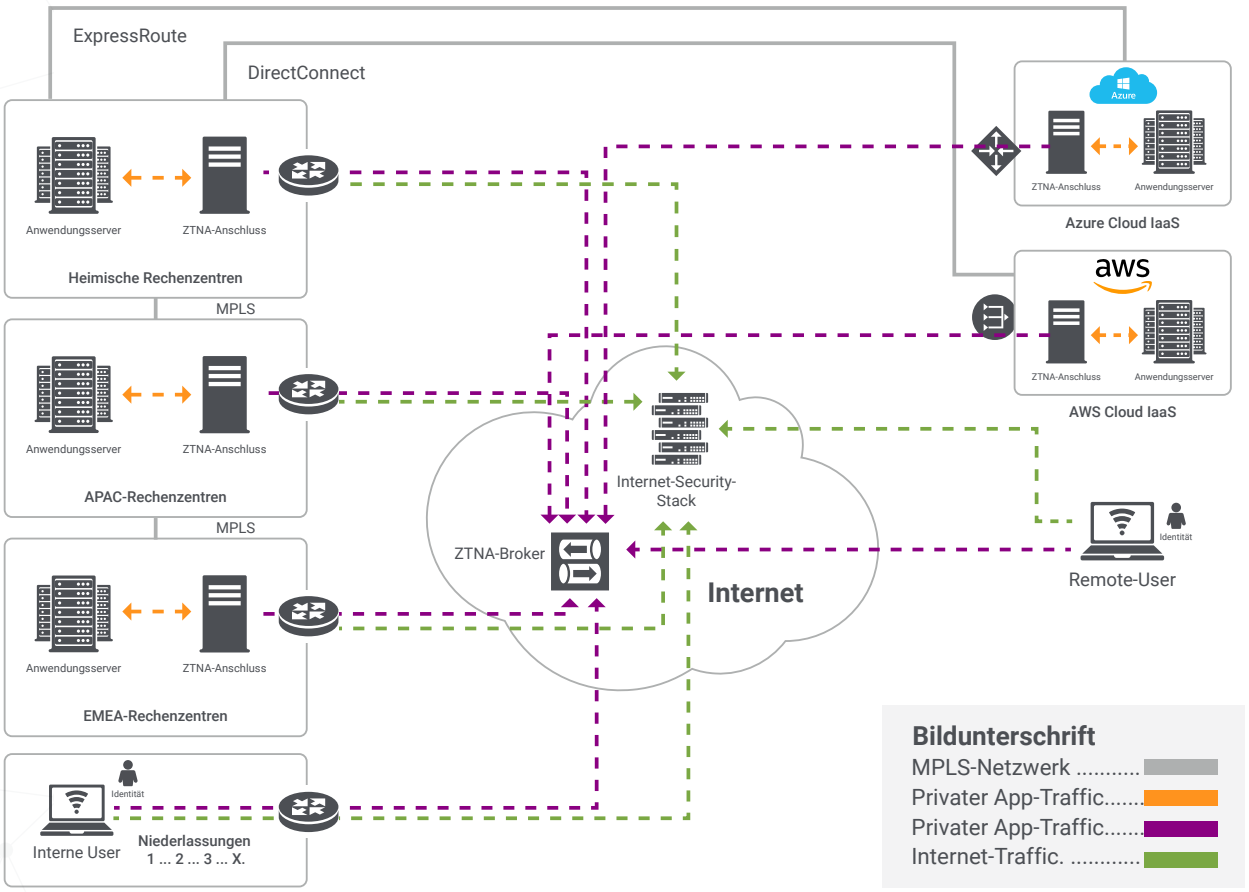
02 Der gesamte Internet-Traffic der Remote - User wird ins Rechenzentrum zurückgeleitet, wo er durch den (Hardware) Security-Stack der Organisation untersucht wird. Dieses so genannte Full Tunnel VPN ist zwar ideal für Sicherheitsteams, die gewährleisten müssen, dass die Benutzer sicher sind, wenn sie sich außerhalb des Unternehmensnetzwerks befinden, kann jedoch die Nutzererfahrung negativ beeinträchtigen, wenn alle Internet-/SaaS-Anwendungen erst einmal wieder zurückgeleitet werden müssen, anstatt lokale Ausgänge nutzen zu können. Viele Benutzer haben jetzt zu Hause Breitband-Internetanschlüsse, die schneller sind als einige Unternehmens-WAN-Anschlüsse (selbst im ländlichen Tennessee habe ich über meinen ISP eine Glasfaserverbindung mit 1 Gbit/s).

03 Interne User hängen in der Regel - kabelgebunden oder drahtlos - an Geräte-/User-Netzwerken, können aber meist trotzdem Verbindungen zu allen Rechenzentren-Netzwerken herstellen, da diese Netzwerke für gewöhnlich als "vertrauenswürdig" gelten. Der Zugriff auf interne Anwendungen wird über das LAN geroutet, und Internet- / SaaS-Anwendungen durchlaufen das Security-Stack, bevor sie an den ISP weitergeleitet werden. Problematisch an dieser Situation ist die falsche Annahme, dass Sie automatisch allen Benutzern und Geräten vertrauen können, nur weil Sie das Netzwerk "besitzen" und kontrollieren.

Beachten Sie, dass für den Remote-Zugriff zunächst der eingehende Zugang aus dem Internet (VPN) notwendig ist, und interne User die Möglichkeit haben müssen, unabhängig von ihrer Identität, direkt mit allen Anwendungsservern zu kommunizieren.

Eine Referenzarchitektur für den Zugriff auf interne Apps ohne erhöhtes Risiko

Letztendlich ist das Ziel einer softwaredefinierten Architektur die Entkopplung des Anwendungszugriffs vom Netzwerkzugriff. Benutzer müssen nicht mehr im Netzwerk platziert werden, private Anwendungen sind nur für autorisierte Benutzer zugänglich; IP-Adressen sind nicht mehr dem Internet ausgesetzt und die Komplexität der Verwaltung von Netzwerksegmenten, FW-Richtlinien und ACLs nimmt ab. Die folgende Abbildung gewährt einen vereinfachten Blick auf das Endergebnis.



Bei dieser neuen, softwaredefinierten Architektur werden Sie feststellen, dass es eine klare Trennung zwischen Rechenzentrums-/Anwendungsnetzwerken, Remote-Usern und internen Usern gibt. Es spielt keine Rolle, ob Ihr Unternehmen nur zwei heimische Rechenzentren, ein Dutzend globale Rechenzentren, einige Azure- /AWS-/GCP-Umgebungen usw. hat. Die Ergebnisse sind relativ klar:

01

Private Netzwerke, wie MPLS oder sogar Site-to-Site-VPNs, sollten zwischen Rechenzentren und Cloud IaaS-Umgebungen nur dort notwendig sein, wo eine Server-zu-Server-Kommunikation erforderlich ist. Wenn Ihre Organisation die www-Webschicht der Website auf AWS verschoben hat, sich die Backend-SQL-Datenbank jedoch noch in einem physischen Rechenzentrum befindet, benötigen Sie weiterhin eine private Konnektivität (geringe Latenz, hohe Bandbreite) zwischen diesen Standorten.

02 Der Remote-Zugriff erfordert keine eingehende Konnektivität mehr für Benutzer, wie z.B. vpn.company.com. Diese Architektur verlegt die Orchestrierungsebene (Steuerungsebene) in die Cloud, wo die Kommunikation von Benutzern beendet wird. Die Gateways, in der Zscaler-Welt als ZPA App-Konnektoren bezeichnet, benötigen weder eingehende Überwachungsports noch einen öffentlichen IP-/DNS-Eintrag. Diese Konnektoren kommunizieren ausgehend über TLS mit der SaaS-basierten Orchestrierungsebene. Interne Anwendungen werden erst vermittelt, wenn die Identität eines Benutzers überprüft und mit den Zugriffsrichtlinien abgeglichen wurde.

- Wenn der Zugriff eines Benutzers auf eine interne Anwendung / Ressource autorisiert wurde, fügt die Orchestrierungsebene die ausgehenden TLS-Verbindungen zwischen den Konnektoren und den User-Geräten zusammen. Weil dieser Benutzer jedoch nicht im Netzwerk platziert wird, bleiben die DNS-basierten Anwendungen verschleiert. Dies bedeutet, dass die tatsächlichen privaten IP-Adressen von Anwendungsservern nicht für die Benutzergeräte sichtbar sind. Vielmehr wird auf dem Client für jeden App-Zugriff dynamisch eine synthetische IP-Adresse erstellt.

- Wenn ein Benutzer keinen Zugriff auf eine interne Anwendung erhält, entfällt auch jeglicher Netzwerk-Traffic in Richtung Rechenzentrum. Die Anforderung wird bereits in der Cloud blockiert, ohne dass ein Risiko entsteht, dass Benutzer bis an die „Haustür" kritischer Anwendungsserver gelangen. Das lässt sich am einfachsten bewerkstelligen, indem man Benutzer in der Cloud abkoppelt, bevor sie eine SSH- oder RDP-Sitzung mit einem Server einrichten können. Auch wenn ein Benutzer die SSH-/RDP-Sitzung höchstwahrscheinlich nicht authentifizieren kann (von einem Brute-Force-Angriff oder gestohlenen Anmeldeinformationen einmal abgesehen), beseitigt diese Architektur dieses Risiko. Und was ist das Beste daran? Alle diese Versuche werden protokolliert, sodass Ihre Sicherheitsorganisation proaktiv (und reaktiv) überwachen kann, was Benutzer zu tun versuchen. So könnte man beispielsweise alle Protokolle an Ihr SIEM, z. B. Splunk, senden und eine Warnmeldung für den Fall erstellen, dass ein Benutzer eine Anzahl X blockierter Richtlinien in X Minuten auf denselben Servern/Ports generiert; beispielsweise versucht der Benutzer innerhalb von 5 Minuten 20-mal, über SSH in sap.company.com zu gelangen. Wenn der Benutzer über eine Policy blockiert wird, sind Sie sicher und können proaktiv feststellen, ob das Gerät des Benutzers gefährdet ist oder der Benutzer böswillige Absichten hatte. Wurde der Benutzer nicht über eine Policy blockiert, erfolgte zwar eine Vermittlung der SSH-Sitzung, aber der Server lehnte falsche Anmeldeinformationen ab. Dies bedeutet, dass dieser Benutzer autorisiert wurde, aber das Administratorkennwort (root) vergessen hatte.

03 Alle User-Netzwerke sollten wie Internetcafés oder Gast-WLANs behandelt werden. Ob sich ein Benutzer auf dem Hauptcampus der Zentrale, in einer Niederlassung, in einer Produktionsstätte oder einfach auf Reisen befindet – es sollte keinen Grund geben, den Benutzer im Netzwerk zu platzieren und ihm die Möglichkeit zu geben, Ihre Anwendungsserver und Rechenzentren zu erkunden/anzusteuern. Hier sollte unbedingt beachtet werden, dass manche Niederlassungen, abgesehen von User-Zugriffen auf Anwendungen, noch weitere Anforderungen stellen. In einem solchen Fall wären für IoT-Geräte und die Server-zu-Server-Kommunikation weiterhin private Netzwerkverbindungen notwendig. Hier ist es am besten, diese Netzwerke von den User-Netzwerken zu trennen.

04 Der Internetzugang - oder Security-Stack - sollte ebenfalls modernisiert werden, um optimale Sicherheit und eine exzellente Nutzererfahrung zu gewährleisten. Wenn Sie die Benutzer vom Netzwerk entkoppeln, sollten Sie nach Möglichkeiten suchen, den Internet-Traffic direkt von den Benutzern aus anstatt zur Überprüfung an ein zentrales Rechenzentrum senden. Bei Zweigniederlassungen kann der gesamte Internet-Traffic über einen vorhandenen Router, eine Firewall oder ein SD-WAN-Gerät an eine Cloud-Sicherheitslösung wie die Zscaler Internet Access-Plattform weitergeleitet werden. Das komplette Security-Stack wird als Service angeboten. Bei über 100 Standorten weltweit, können Sie den Traffic aller Unternehmensstandorte zur Überprüfung an die nächstgelegenen Zscaler-Standorte senden. Sogar, wenn ein Benutzer auf Reisen ist, leistet der einheitliche Zscaler App-Client, ein leichtgewichtiger Weiterleitungsagent, der auf mobilen User-Geräten und Laptops installiert wird, gute Dienste. Er liefert die gewünschte Nutzererfahrung, indem er jedes Backhauling vermeidet und den Internet-Traffic an den nächstgelegenen Zscaler-Knoten leitet, bietet dem IT-Team trotzdem die erforderlichen Sicherheitskontrollen und Transparenz.

Einführung einer ZTNA-Architektur in drei verschiedenen Phasen

Netzwerkarchitekten fragen oft: "Wo fangen wir am besten an?" Eine meiner Lieblingsantworten lautet: "Es kommt darauf an." Ich weiß, dass viele Ingenieure und Architekten dies verstehen, denn es gibt viele mögliche Ergebnisse, die man je nach den spezifischen Bedürfnissen, Anforderungen und Konfigurationen anstreben und erreichen kann. Wir sind dafür verantwortlich, Organisationen die für diesen Weg am besten geeigneten Vorgehensweisen zu empfehlen. Ich möchte ausdrücklich darauf hinweisen, dass der in diesem Abschnitt beschriebene Ansatz eines in Phasen unterteilten Weges keineswegs eine konkrete Abfolge darstellt, an die sich jede Organisation halten muss. Es handelt sich vielmehr um einen übergeordneten Ansatz, der unserer Erfahrung nach in vielen Fällen die jeweiligen Anforderungen erfüllen und gleichzeitig die betreffenden Organisation in die Lage versetzen konnte, das Zero-Trust-Netzwerkkonzept zu übernehmen. Vertrauen wird niemals impliziert und der Zugriff kann adaptiv, auf kontextbezogenen - Benutzer-, Geräte-, Service- usw. Richtlinien basierend erfolgen, die von Administratoren festgelegt wurden.

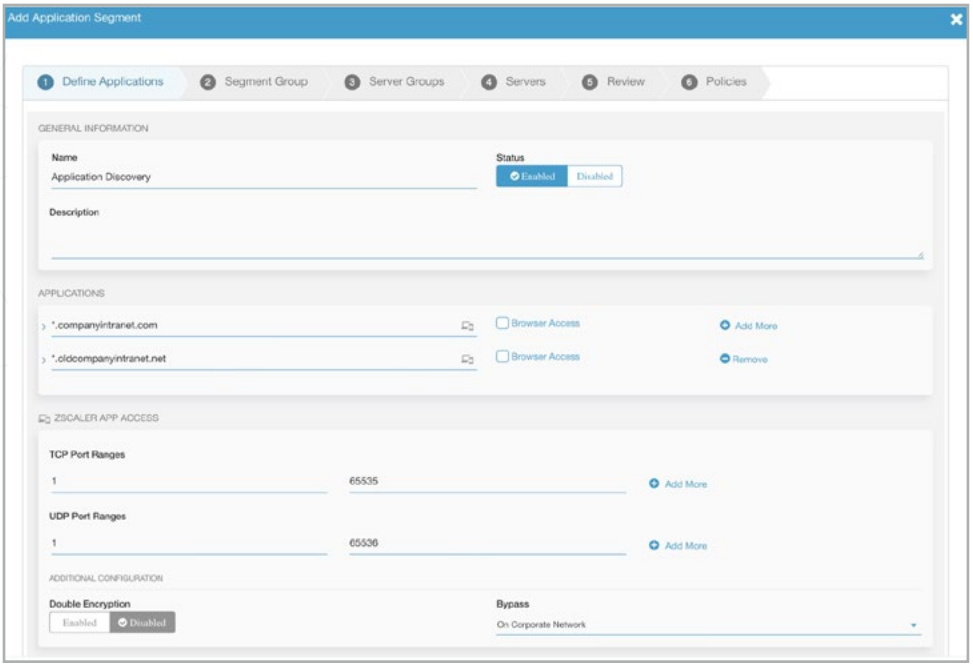
Die einzelnen Schritte sind dabei sehr klein: Beginnen Sie mit Remote-Usern, entwickeln Sie Segmente und nutzen Sie dann ZTNA für den Zugriff auf private Apps für alle Benutzer, unabhängig vom Standort. Sie müssen dabei berücksichtigen, wie Benutzer auf Anwendungen und Services zugreifen und wie Ihre Standorte (Rechenzentren, Cloud IaaS-Umgebungen und physische Standorte, an denen Mitarbeiter arbeiten) verteilt sind (Anzahl und Art). Außerdem müssen Sie alle projektbasierten Zeitpläne berücksichtigen. In vielen Fällen kann eine anstehende VPN-Aktualisierung als eine Art Katalysator fungieren: Anstatt ein VPN der nächsten Generation oder „Always-On"-VPN zu kaufen, das die gleichen Herausforderungen wie Ihr aktuelles VPN mit sich bringt, können Sie auch ZTNA einführen.

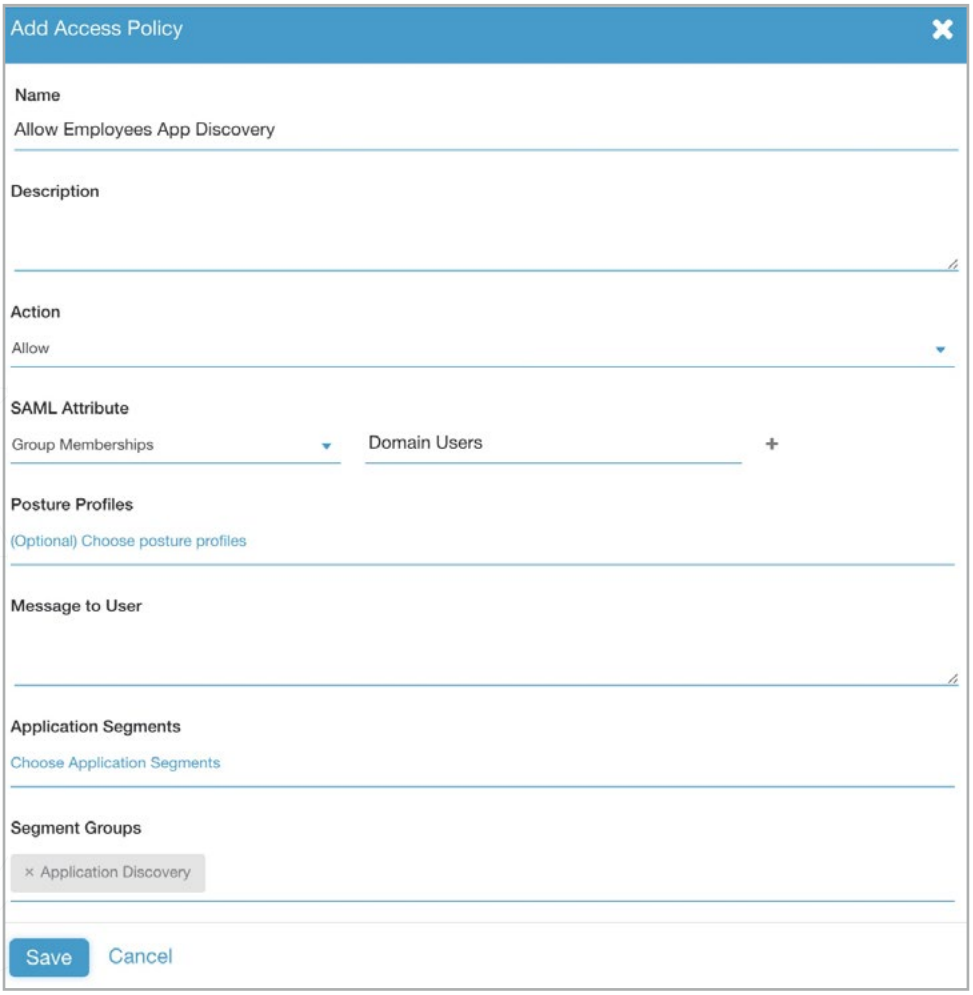
Phase 1 Deployment eines ZTNA für Remote-Zugriff und Anwendungserkennung

In dieser Phase sollten Sie zunächst die vorhandene Remote-Access-VPN-Lösung ersetzen. Dazu müssen Sie möglicherweise das ZTNA mit ähnlichen Zugriffsebenen wie die des aktuellen Remote-Access-VPN bereitstellen. Damit stellen Sie sicher, dass Ihre neue Initiative nicht als bremsender Faktor für die Produktivität der Remote-User betrachtet wird.

Weiterhin müssen Sie wissen, welche privaten Apps in Ihrer Umgebung ausgeführt werden, um die Angriffsfläche zu verringern und Shadow-IT zu beseitigen. Es ist gut möglich, dass weitaus mehr Apps in Ihrer Umgebung ausgeführt werden, als Sie denken. Unsere Lösung mit dem Namen Zscaler Private Access (ZPA) löst dieses Problem mithilfe unserer Application Discovery-Funktion. Sie können unmöglich alle internen Anwendungen oder Services kennen, auf die Ihre Benutzer zugreifen müssen. Mit Application Discovery können Sie also im Wesentlichen Platzhalter wie * .company.com, * .company.net nutzen, alle TCP und UDP-Ports.

Sobald sich ein Benutzer erfolgreich bei dem Service registriert hat, erkennt der Client automatisch, wenn sich der Benutzer nicht mehr im Unternehmensnetzwerk befindet. Alle internen Anwendungen passieren jetzt den ZTNA, wenn sich der Benutzer nicht im Netzwerk befindet. Es ist kein Start eines VPN-Clients notwendig und der Benutzer kann wie zuvor auf interne Ressourcen zugreifen. Alle diese Zugriffsprotokolle befinden sich auf der ZPA-Administratorkonsole und können auch nahezu in Echtzeit an das SIEM Ihrer Wahl gestreamt werden, sodass Sie einen genauen Einblick haben, auf welche Anwendungen Benutzer zugreifen.





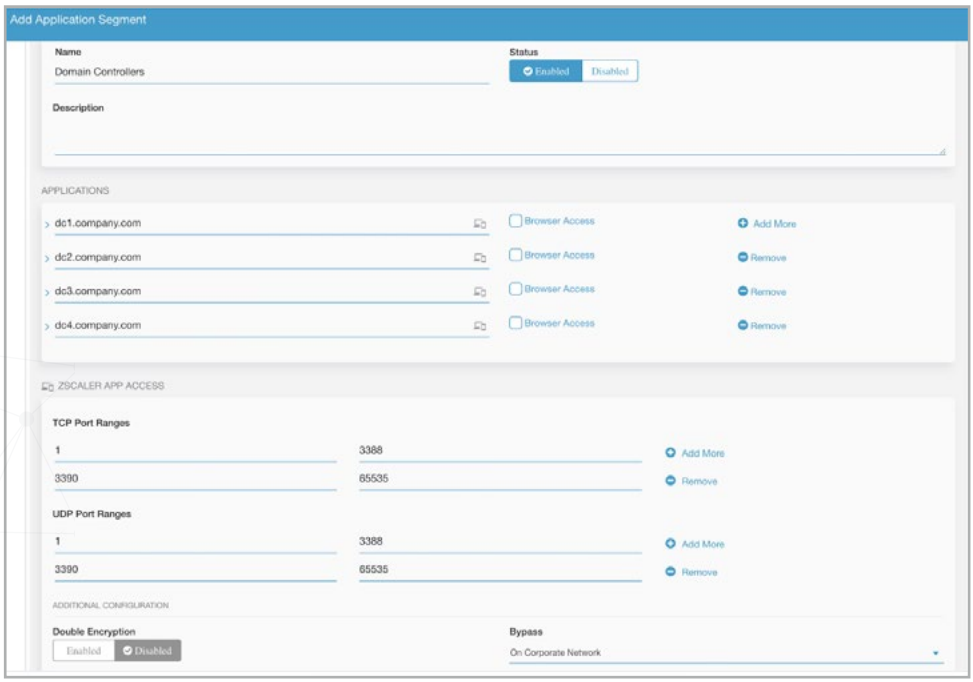
Da das interne private Netzwerk (MPLS, Site-to-Site-VPN) höchstwahrscheinlich noch besteht, beendet der Zscaler App-Client ZPA automatisch, sobald der Benutzer zum Unternehmensnetzwerk zurückkehrt. Jetzt erfolgt der gesamte Zugriff auf interne Anwendungen im LAN, ohne Zscaler im Pfad.

Phase 2

Nutzen Sie die Mikrosegmentierung, um die Konnektivität nach dem Prinzip der geringsten Rechte sicherzustellen.

In dieser Phase müssen Sie Policies definieren, die private Anwendungen in Segmente unterteilen und über Benutzeridentitätsattribute Zugriff auf diese Segmente gewähren.

Da große Organisationen möglicherweise über Hunderte oder Tausende einzigartiger Anwendungen/Services verfügen, möchten viele Organisationen möglicherweise zunächst Verwaltungsports wie TCP 22 (SSH) und TCP / UDP 3389 (RDP) segmentieren und IT-Benutzern nur globalen Zugriff auf diese Ports gewähren. Natürlich kann es immer einmalige Anforderungen geben, aber diese Segmentierung kann dazu beitragen, die Anzahl der Benutzer zu verringern, die eine Verbindung zu Servern herstellen, auf die sie überhaupt nicht erst zugreifen können sollten. Beispielsweise sollten Ihre Vertriebsmitarbeiter eher nicht in der Lage sein, auf einem Windows Server, der Ihre SAP-Anwendung hostet, auf TCP 3389 zuzugreifen. Sie sollten nur zum Front-End-Webabschnitt gelangen, bei dem es sich um dieselben Server handelt, jedoch nur an die Ports TCP 80/443.



Im Idealfall können Infrastruktur-Server, bei denen es sich um Domänencontroller/-Services, Sicherheitssoftware-Clients, Softwarebereitstellungs-Clients usw. handeln kann, leicht segmentiert werden, da die Hosts bekannt sind.

Die App-Segmentierung ist ein fortlaufender Prozess. Eine allgemeine Empfehlung lautet, Anwendungen zu priorisieren, die für das Unternehmen am wichtigsten sind und die nur bekannten User-Typen zugänglich sein sollten.

Beim Segmentieren der Anwendungen, werden diese aus dem "Pool" zur Anwendungserkennung entfernt. Dies bedeutet, dass Sie frei kombinieren können, um sicherzustellen, dass Benutzer weiterhin auf nicht explizit definierte Anwendungen in Ihren Domänen, aber auch auf bekannte Anwendungen an den erforderlichen Service-Ports zugreifen können.

HINWEIS: Vergessen Sie dabei nicht die Internetsicherheit!

Wir konzentrieren uns in diesem Leitfaden zwar auf die privaten Anwendungen, aber Sie müssen sich darüber im Klaren sein, dass es ebenso wichtig ist, ein Security-Stack für den gesamten Internet-Traffic bereitzustellen. Viele Organisationen interessieren sich für einen moderneren Inbound- und Outbound-Security-Stack, der vollständig Cloud-basiert ist, anstatt sich auf Appliances oder virtuelle Appliances (d.h. Firewalls) zu verlassen. Die Outbound-Cloud-Sicherheitslösung von Zscaler heißt Zscaler Internet Access (ZIA).

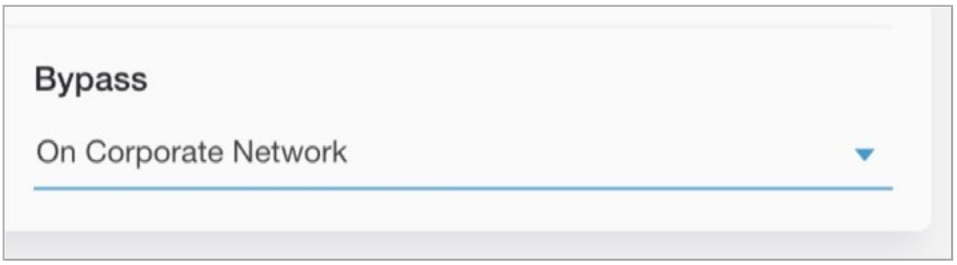
Phase 3 ZTNA für den Zugriff auf private Apps für alle Benutzer (nicht nur Remote-User)

Sie sind nun bereit für die letzte Phase. Dies bedeutet, dass der Zugriff auf private Anwendungen in Zukunft auf genauen Einstellungen basiert, die standardmäßig nur explizite Konnektivität nach dem Prinzip der geringsten Rechte ermöglichen.

ZPA ermöglicht dies durch Inside-Out-Konnektivität über doppelt verschlüsselte TLS-Mikrotunnel, die pro Sitzung eingesetzt werden und ein sicheres Segment zwischen einem autorisierten Benutzer und einer bestimmten privaten App erstellen.

Sie erinnern sich vielleicht, dass ich bereits erwähnt habe, wie Zscaler App das Unternehmensnetzwerk erkennen kann. Dies bedeutet, dass in ZPA jedes Anwendungssegment die folgenden Konfigurationsoptionen aufweist: (1) ZPA im Unternehmensnetzwerk zu umgehen, (2) ZPA immer zu umgehen oder (3) ZPA nie zu umgehen. In Phase 1 haben Sie App-Segmente mit Option 1 bereitgestellt. Doch wie sieht es aus, wenn es nicht nur um den sicheren Zugriff der Remote-User, sondern aller Benutzer geht? Dazu können Sie einfach die App-Segmente auf die Option schalten, die vorschreibt, ZPA niemals zu umgehen. Damit wird der gesamte Zugriff auf interne Ressourcen über diese explizite Vertrauensarchitekturlösung vermittelt, selbst wenn sich die Benutzer in einem Büro befinden, und niemals nur im LAN direkt an die Anwendungsserver in Ihrem Rechenzentrum weitergeleitet.

Von



Zu

Das ist doch wunderbar einfach, oder? Ich denke, die mit diesem Wechsel verbundenen Herausforderungen, bleiben außerhalb unserer Plattform. Wie Sie sich vielleicht erinnern, besteht das letztendliche Ziel normalerweise darin, die Anwendungsserver-/Rechenzentrumsnetzwerke vollständig aus allen User-Netzwerken zu entfernen. Dies bedeutet keine Konnektivität von Niederlassungen, Produktionsstätten usw. (um genau zu sein, keine Konnektivität von den USER-Netzwerken an diesen Standorten) zum Rechenzentrum.

Letzte Überlegungen und Profi-Tipps:

Es ist unter Umständen am einfachsten, mit einem neuen kleinen Büro zu beginnen, das noch nicht ins Netzwerk integriert ist. Statten Sie dieses Büro nur mit einer Breitband-Internetverbindung aus. Leiten Sie den gesamten Internet-Traffic zu einer Cloud-Sicherheitsplattform (z. B. ZIA) und lassen Sie den Traffic der privaten Anwendungen über die ZPA-Plattform laufen.

Betrachten Sie das neue Büro, als sei es ein Internetcafé. Berücksichtigen Sie dabei immer, dass wir heute auf diese Weise Benutzer mit Anwendungen verbinden können. Einige Standorte, wie Produktionsstätten mit Sensoren, IoT-Geräten und Servern, müssen wahrscheinlich weiterhin über ein privates MPLS oder VPN mit Ihren Rechenzentren kommunizieren. Behandeln Sie diese Standortnetzwerke als Rechenzentren und nehmen Sie nur die Benutzer davon aus. Alle Benutzer erhalten "Gast-WLAN"-Status, und der interne Anwendungszugriff wird über Autorisierungen vermittelt.

Trotz aller Aufregung und Begeisterung im Hinblick auf ZTNA-Architekturen, besteht das eigentliche Ziel immer noch darin, den Benutzern eine möglichst reibungslose Nutzererfahrung zu bieten und dabei die notwendige Absicherung privater Apps zu gewährleisten. Es wird einige Zeit dauern, bis Ihre Organisation diese neue Methode eingeführt hat, aber Sie als Netzwerkarchitekt können das Fundament (die Plattformen) dafür legen.

Erleben Sie ZPA selbst und melden Sie sich unter
https://www.zscaler.com/zpa-interactive
für eine 7-tägige gehostete Testversion an.

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA
+1 408 533 0288
www.zscaler.com